Number Theory Section Summary: 3.3

The Goldbach Conjecture

1. Summary

We now can prove that the primes are infinite in number, and we have no doubt sensed the feeling that their distribution is uneven (since so many appear in the first 10 natural numbers, and then start to get annihilated in the spiraling patterns of the sieve of Eratosthenes). But what can we say about the distribution of primes? Are there interesting patterns? This section seeks to sum up some of what we know.

Various famous interesting conundrums, mysteries, conjectures, etc. are discussed, including

- The Goldbach Conjecture (that every even $n > 2$ is the sum of two primes);
- Twin Primes, and other gaps between primes;
- Dirichlet's theorem about primes of the form $a+kb$, with $\gcd(a,b) = 1$; and
- Primes of various forms given by the division algorithm.

2. Definitions

Twin primes: prime pairs of the form p, $p+2$.

Euler polynomial: $f(n) = n^2+n+41$ (which produces primes for the integers from 0 to 39). (Euler showed that it did not generate primes for all n, which others apparently believed.)

$n = 41$

$41^2 + 41 + 41$

Examples: other gaps in primes:

- Exercise #3, p. 59 – one minute!

Find all pairs of primes p & q satisfying $p - q = 3$.

2 & 5!

One even, one odd.

- Exercise #9a, p. 59 – *Use* ~~*6k+k*~~ $\quad n, n+2, n+4$ can't all be prime for $n > 3$.

If n were $6k+1$, then $\overbrace{6k+3}^{\text{divisible by } 3}$ & $6k+5$

$6k+3$ it wouldn't be prime $(k>0)$

$6k+5$, then $6k+7$ & $6k+9$

$6(k+1)+1 \qquad \underbrace{6(k+1)+3}_{\text{divisible by } 3}$

- Exercise #9b, p. 59 – *prime-triplets* – use the sieve, or Mathematica!

- Arbitrary long, primeless gaps.

Suppose you want a gap of size n

$n > 1$

$$\left.\begin{array}{ll} n!+2 & 2 \mid \text{it} \\ n!+3 & 3 \mid \text{it} \\ \vdots & \vdots \\ n!+n & n \mid \text{it}. \end{array}\right\} \text{gap of } n-1$$

For a gap of n, take $n+1$:

$$(n+1)!+2, \ldots, (n+1)!+(n+1)$$

3. Theorems

Goldbach Conjecture (unproven yet heavily favored: hence, still a conjecture): Every even $n > 2$ is the sum of two primes.

$8 = 5+3$

$22 = 11+11$
$= 5+17$

Note: it's interesting that it's been shown (Vinogradov) that

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0$$

where $A(x)$ is the number of evens less than or equal to x and not expressible as the sum of two primes. ($A(x)$ may be zero for all x!) This means that "almost all" integers satisfy the conjecture. *What does that mean?!* ("The Goldbach conjecture is false for at most 0% of all even integers; this *at most* 0% does not exclude, of course, the possibility that there are infinitely many exceptions." George Landau)

See ping pong below....

Twin Prime Conjecture: There are infinitely many twin primes.

Lemma: The product of two or more integers of the form $4n+1$ is of the same form.

Theorem 3.6: There are infinitely many primes of the form $4n+3$.

Example: Exercise #13, p. 60 asks us to show the same thing for integers of the form $6n+5$.

Lemma: product of $6k+1$ integers is of the same form.

Proof: $(6k+1)(6l+1) = 6^2kl + 6(k+l)+1 = 6[\ \ ]+1$ ✓

Theorem: There are infinitely many primes of form $6k+5$.

By contradiction, assume not: let $S = \{q_1, \ldots, q_r\}$ be the set of primes of form $6k+5$.

Consider $N = 6q_1\cdots q_r - 1 = 6[q_1\cdots q_r - 1]+5$

$N > q_i \;\forall i$, & of the form $6k+5$; if it's prime we have a contradiction, since $N \notin S$.

Let $N = p_1 \cdots p_s$ be the prime factorization of composite N. $p_i \neq 2$ or 3; N is odd, and of the form $6k+5$ – the first rules out 2, the second rules out 3 (since N would be of form $6k+3$).

If all p_i were of the form $6k+1$, then N would be too by the lemma. Hence at least one is of form $6k+5$; i.e. $p_i = q_j$ for some i, j. But $p_i \mid N$ and $p_i \mid 6q_1 \cdots q_r$, so $p_i \mid (N - 6q_1 \cdots q_r) = -1$ – contradiction.

Hence there are infinitely many of form $6k+5$.

Theorem 3.7 (Dirichlet): If a and b are relatively prime positive integers, then the arithmetic progression

$$a,\ a+b,\ a+2b,\ a+3b, \ldots$$

contains infinitely many primes.

Theorem 3.8: If all the $n > 2$ terms of the arithmetic progression

$$p,\ p+d,\ p+2d,\ \ldots, p+(n-1)d$$

are prime numbers, then the common difference d is divisible by every prime $q < n$.

Ping Pong Ball Conundrum: a barrel, and ping pong balls numbered 1, 2, ... – one for each natural number. You have one minute. In the first 30 seconds,

① Put 10 in, those numbered 1-10, then draw out ball #1. In the next 15 seconds,

② Put the next ten in, 11-20, & draw out #2.

Continue in this fashion, cutting the interval in half until the minute is up.

Question: how many balls are in the barrel?

Answer: 0! Every ball came out:

Ball #1	came out	at		$1-\frac{1}{2}$	minute
#2	"	"	"	$1-(\frac{1}{2})^2$	"
#3	"	"	"	$1-(\frac{1}{2})^3$	"
⋮				⋮	
#n	"	"	"	$1-(\frac{1}{2})^n$	"

It's a miracle! We put them in ten times as fast as we pulled them out, but in the end they were all gone....